Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A smartcard transaction system configured with a biometric security system, said system comprising:
a smartcard configured to communicate with a reader;
a reader configured to communicate with said system;
a biometric sensor configured to detect a first proffered biometric sample and a second proffered biometric sample, said biometric sensor configured to communicate with said system; and,
a device configured to verify said proffered biometric samples to facilitate a transaction.

[c2] The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3] The smartcard transaction system of claim 1, wherein said biometric sensor is configured to facilitate a finite number of scans.

[c4] The smartcard transaction system of claim 1, wherein said biometric sensor is configured to log at least one of detected biometric samples, processed biometric sam-

ples and stored biometric samples.

[c5] The smartcard transaction system of claim 1, further including a database configured to store a data packet, wherein said data packet includes at least one of proffered and registered biometric samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The smartcard transaction system of claim 4, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c7] The smartcard transaction system of claim 5, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The smartcard transaction system of claim 1, further including a device configured to compare at least one of a first proffered biometric sample with a second proffered biometric sample, a first proffered biometric sample with a stored biometric sample, and a second proffered biometric sample with a stored biometric sample.

[c9] The smartcard transaction system of claim 8, wherein said device configured to compare a biometric sample is at least one of a third-party security vendor device and

local CPU.

[c10] The smartcard transaction system of claim 8, wherein a stored biometric sample comprises a registered biometric sample.

[c11] The smartcard transaction system of claim 10, wherein said registered biometric sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c12] The smartcard transaction system of claim 11, wherein different registered biometric samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c13] The smartcard transaction system of claim 11, wherein a biometric sample is primarily associated with first user information, wherein said first information comprises at

least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a biometric sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

[c14] The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered biometric sample.

[c15] The smartcard transaction system of claim 1, wherein said smartcard is configured to detect said second proffered biometric sample upon rejection of said first proffered biometric sample.

[c16] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c17] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c18] A method for facilitating biometric security in a smartcard transaction system comprising:
proffering a first biometric to a biometric sensor to initiate verification of a first biometric sample for facilitating authorization of a transaction and wherein said sensor is communicating with said system; and
proffering a second biometric to a biometric sensor to initiate verification of a second biometric sample for facilitating authorization of a transaction and wherein said sensor is communicating with said system

[c19] The method of claim 18, further comprising registering at least two biometric samples with an authorized sample receiver.

[c20] The method of claim 19, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a first biometric to said

authorized sample receiver, processing said first biometric to obtain a first biometric sample, associating said first biometric sample with user information, verifying said first biometric sample, and storing said first biometric sample upon verification.

[c21] The method of claim 19, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a second biometric to said authorized sample receiver, processing said second biometric to obtain a second biometric sample, associating said second biometric sample with user information, verifying said second biometric sample, and storing said second biometric sample upon verification.

[c22] The method of claim 18, wherein said steps of proffering a first and second biometric further include proffering a first and second biometric to a biometric sensor to initiate at least one of: storing, comparing, and verifying said first and second biometric samples.

[c23] The method of claim 18, wherein said steps of proffering a first and second biometric to a biometric sensor to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard

system.

[c24] The method of claim 18, wherein said steps of proffering a first and second biometric to a biometric sensor communicating with said system, to initiate verification further includes comparing at least one of: a first proffered biometric sample with a second biometric sample, a first proffered biometric sample with a stored biometric sample, and a second proffered biometric sample with a stored biometric sample.

[c25] The method of claim 24, wherein said step of comparing includes comparing at least one of: a first proffered biometric sample with a second biometric sample, a first proffered biometric sample with a stored biometric sample, and a second proffered biometric sample with a stored biometric sample further includes using at least one of a third-party security vendor device and local CPU.

[c26] The method of claim 18, wherein said steps of proffering a first and second biometric to a biometric sensor to initiate verification further includes the use of at least one secondary security procedure.

[c27] A method for facilitating biometric security in a smartcard transaction system comprising:

detecting a first proffered biometric at a sensor to obtain a first proffered biometric sample, wherein said sensor communicates with said system;
verifying the first proffered biometric sample;
detecting a second proffered biometric at a sensor to obtain a second proffered biometric sample, wherein said sensor communicates with said system;
verifying the second proffered biometric sample; and
authorizing a transaction to proceed upon verification of at least one of said first and second proffered biometric samples.

[c28] The method of claim 27, wherein said steps of detecting further include detecting a first and second proffered biometric via at least one of a smartcard, reader, and network.

[c29] The method of claim 27, wherein said steps of detecting further include at least one of: detecting, storing, and processing a first and second proffered biometric sample.

[c30] The method of claim 27, wherein said steps of detecting further include receiving a finite number of proffered biometric samples during a transaction.

[c31] The method of claim 27, wherein said steps of detecting

further include logging each proffered biometric sample.

[c32] The method of claim 27, wherein said step of verifying includes comparing at least one of: a first proffered biometric sample with a second biometric sample, a first proffered biometric sample with a stored biometric sample and a second proffered biometric sample with a stored biometric sample.

[c33] The method of claim 32, wherein said step of comparing includes comparing at least one of: a first proffered biometric sample with a second biometric sample, a first proffered biometric sample with a stored biometric sample and a second proffered biometric sample with a stored biometric sample includes comparing a proffered biometric sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember

[c34] The method of claim 27, wherein said step of verifying includes verifying a first and second proffered biometric sample using information contained on at least one of a local database and a remote database.

[c35] The method of claim 27, wherein said step of verifying includes verifying a first and second proffered biometric sample using at least one of a local CPU and a third-party security vendor.